IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TAASERA LICENSING LLC,	§	
	§	
Plaintiff,	§	Case No. 2:23-cv-00113-JRG
	§	
v.	§	
	§	
PALO ALTO NETWORKS, INC.,	§	
	§	
Defendant.	§	

DEFENDANT PALO ALTO NETWORKS, INC.'S
PARTIAL MOTION TO DISMISS UNDER
FEDERAL RULE OF CIVIL PROCEDURE 12(b)(6)

TABLE OF CONTENTS

Page

I. The asserted claims of the '796 patent are patent-ineligible under § 101. 2

A. *Alice* step one: the asserted claims are directed to the abstract idea of identifying and extracting information by matching a pattern.....2

B. *Alice* step two: the asserted claims fail to recite an inventive concept. 5

II. The asserted claims of the '356 patent are patent-ineligible under § 101. 6

A. *Alice* step one: the asserted claims are directed to the abstract idea of sorting packets of data based on simple if/then logic that was performed by humans. 6

B. *Alice* step two: the asserted claims fail to recite an inventive concept. 9

III. The asserted claims of the '517 patent are patent-ineligible under § 101. 10

A. *Alice* step one: the asserted claims are directed to the abstract idea of assigning a score based on risk using rules and policies that are generic and undefined. 10

B. *Alice* step two: the asserted claims fail to recite an inventive concept. 12

IV. The asserted claims of the '038 and '918 patents are patent-ineligible under § 101.....12

A. *Alice* step one: the asserted claims are directed to the abstract idea of determining compliance with a policy and restricting access to resources. 12

B. *Alice* step two: the asserted claims fail to recite an inventive concept. 15

TABLE OF AUTHORITIES

Page(s)

Cases

Affinity Labs of Texas, LLC v. Amazon.com, Inc.,
838 F.3d 1266 (Fed. Cir. 2016).....8

Alice Corp. v. CLS Bank Int'l,
573 U.S. 208 (2014)..... *passim*

Cisco Sys., Inc. v. Uniloc 2017 LLC,
813 F. App'x 495 (Fed. Cir. 2020) 11

Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n,
776 F.3d 1343 (Fed. Cir. 2014).....3, 5, 6

Credit Acceptance Corp. v. Westlake Servs.,
859 F.3d 1044 (Fed. Cir. 2017).....7

Customedia Techs., LLC v. Dish Network Corp.,
951 F.3d 1359 (Fed. Cir. 2020).....4, 8

DDR Holdings, LLC v. Hotels.com, L.P.,
773 F.3d 1245 (Fed. Cir. 2014).....4, 14

Dropbox, Inc. v. Synchronoss Technologies, Inc.,
815 F. App'x 529 (Fed. Cir. 2020) 11

Elec. Power Grp., LLC v. Alstom S.A.,
830 F.3d 1350 (Fed. Cir. 2016).....2, 4, 11

Enfish, LLC v. Microsoft Corp.,
822 F.3d 1327 (Fed. Cir. 2016).....4, 14

Ericsson Inc. v. TCL Commc'n Tech. Holdings Ltd.,
955 F.3d 1317 (Fed. Cir. 2020).....12, 13, 14

In re Gale,
856 F. App'x 887 (Fed. Cir. 2021) 14

Intellectual Ventures I LLC v. Erie Indemnity Co.,
711 F. App'x 1012 (Fed. Cir. 2017) 8

Intellectual Ventures I LLC v. Symantec Corp.,
838 F.3d 1307 (Fed. Cir. 2016).....4, 7, 13

TABLE OF AUTHORITIES (continued)

Page(s)

SAP Am., Inc. v. InvestPic, LLC,
898 F.3d 1161 (Fed. Cir. 2018)..... *passim*

Smart Sys. Innovations, LLC v. Chicago Transit Auth.,
873 F.3d 1364 (Fed. Cir. 2017).....11

SmartGene, Inc. v. Advanced Biological Labs., SA,
555 F. App'x 950 (Fed. Cir. 2014) 11

In re: Taasera Licensing LLC, Patent Litig.,
No. 2:22-MD-03042-JRG, Dkt. No. 178 .....1, 2

Statutes

35 U.S.C. § 101..... *passim*

Other Authorities

Fed. R. Civ. P. 12(b)(6).....1

This action involves nine patents that purportedly relate to network security systems. Although all asserted claims of all nine patents are invalid, this motion focuses on the asserted claims of five patents that are so clearly abstract that their patent-ineligibility can, and should, be resolved on the pleadings, which will substantially streamline this case. Palo Alto Networks, Inc. ("PAN") thus moves for partial dismissal under Federal Rule of Civil Procedure 12(b)(6) because all asserted claims of the following patents are ineligible under 35 U.S.C. § 101: Nos. 6,842,796 (the "'796 patent"), 8,127,356 (the "'356 patent"), 8,850,517 (the "'517 patent"), 8,955,038 (the "'038 patent"), and 9,923,918 (the "'918 patent") (collectively, the "challenged patents").[1]

The parties briefed and orally argued these issues on February 21, 2023, in a declaratory judgment action brought by PAN that was consolidated for MDL proceedings before this Court. Because the Court dismissed PAN's declaratory judgment complaint on jurisdictional grounds, the Court did not reach the merits of PAN's § 101 motion. *See In re: Taasera Licensing LLC, Patent Litig.*, No. 2:22-MD-03042-JRG ("MDL"), Dkt. No. 178 at 24–25. Now that Taasera has refiled suit against PAN, PAN files this motion to reassert its § 101 arguments on the same grounds.

As shown below, all asserted claims of the five challenged patents fail both steps of the *Alice* inquiry and are patent-ineligible under § 101 because they are (1) directed to abstract ideas and (2) fail to recite any inventive concept. *See Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217–18 (2014). First, the asserted claims of all five patents are directed to abstract ideas:

- **The '796 patent** claims are all directed to identifying and extracting information by

[1] These patents are attached to Taasera's complaint as Dkt. No. 1-1 ('796 patent), 1-3 ('356 patent), 1-5 ('517 patent), 1-6 ('038 patent), and 1-9 ('918 patent). In its infringement contentions against PAN, Taasera has asserted the following claims of the challenged patents:

- '796 patent: claims 1, 2, 7, 10, 12, 13, 18, 21, and 23–25;
- '356 patent: claims 1–4, 6, 8–10, and 12–20;
- '517 patent: claims 1–5, 12–17, and 24;
- '038 patent: claims 1–33; and
- '918 patent: claims 1–24.

matching a pattern, which is exactly what humans do when reading or skimming a letter, focusing on key words or phrases, and writing them down in notes or records.

- **The '356 patent** claims are all directed to sorting packets of data—i.e., classifying whether packets are "new exploit candidates"—using simple if/then logic that was previously applied by humans and that is analogous to sorting out junk mail.

- **The '517 patent** claims are all directed to assigning a score based on risk, which humans have long done, e.g., when determining credit scores and insurance rates.

- **The '038 and '918 patents**, which are related and share a common specification, recite claims that are all directed to determining compliance with a policy and restricting access to resources (e.g., akin to limiting access to a bridge or highway based on compliance with toll or carpool/HOV requirements).

Second, apart from these abstract ideas, the asserted claims recite nothing beyond "generic computer and network technology," which is "ineligible under § 101." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1356 (Fed. Cir. 2016). Moreover, Taasera has admitted that claim 1 of each challenged patent is representative for § 101 purposes. Ex. A (MDL Hr'g Tr.) at 29:22–24. Thus, Taasera's complaint should be dismissed with respect to each challenged patent.

I. The asserted claims of the '796 patent are patent-ineligible under § 101.

A. *Alice* step one: the asserted claims are directed to the abstract idea of identifying and extracting information by matching a pattern.

The '796 patent, which predates *Alice*, claims nothing more than the abstract idea of identifying and extracting information by matching a pattern—tasks that humans routinely perform when reading a document and focusing on key words or phrases. Indeed, the patent describes "[t]he present invention" as "exploiting the readily-identifiable structure of language to explicitly identify portions of data in a document that a user seeks to be identified, e.g., relevant or important information." Dkt. No. 1-1 at 1:52–55. To do so, the invention uses "regular expressions," i.e., "regularly identifiable or stereotypical phrases that people commonly use to convey particular information." *Id.* at 2:12–17. For example, one can identify a caller's name ("Bob") from the voice message, "Hi John, it's Bob." *Id.* at 2:3–6. The '796 patent admits that "common

programming languages" have "built-in support for regular expressions." *Id*. at 2:11–15, 2:23–27.

Claim 1, which is representative, recites a simple three-step method: (1) identifying a "regularly identifiable expression" that "represents a pattern that is matchable"; (2) identifying a portion of information associated with that expression; and (3) extracting the information:

> 1. A method of automatically processing an input sequence of data symbols, the method comprising the steps of:
> ***identifying*** at least one ***regularly identifiable expression*** in the input sequence of data symbols, wherein the at least one regularly identifiable expression ***represents a pattern that is matchable*** in accordance with a programming language that supports such a regularly identifiable expression;
> ***identifying*** at least ***a portion of information*** associated with the at least one regularly identifiable expression; and
> ***extracting the portion of information***.

Id. at claim 1 (emphasis added). On its face, claim 1 is directed to the abstract idea of identifying and extracting information by matching a pattern. The Federal Circuit has invalidated analogous claims with steps for "1) extracting data from hard copy documents using an automated digitizing unit such as a scanner, 2) recognizing specific information from the extracted data, and 3) storing that information in a memory." *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1345 (Fed. Cir. 2014). Those claims were "drawn to the abstract idea of 1) collecting data, 2) recognizing certain data within the collected data set, and 3) storing that recognized data in a memory." *Id*. at 1347. The Federal Circuit held that such concepts are "undisputedly well-known," and "humans have always performed" them. *Id*. For example, banks have long "reviewed checks, recognized relevant data such as the amount, account number, and identity of account holder, and stored that information in their records." *Id*.

The claims here are no different. Apart from claim 1's reference to a "programming language that supports such a regularly identifiable expression" (Dkt. No. 1-1 at claim 1)—a "generic computer-implemented" limitation—every other limitation refers to activities that can be

"performed by a human, mentally or with pen and paper." *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed. Cir. 2016). "Identifying" and "extracting" is akin to a human recognizing key words like names in a letter and writing them down in a notepad, similar to data-recognition steps that have been held abstract. *See id.* at 1313 ("determining . . . whether [input data] matches a characteristic"); *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1167 (Fed. Cir. 2018) ("selecting certain information" and "analyzing it using mathematical techniques"); *Elec. Power Grp.*, 830 F.3d at 1354 ("gathering and analyzing information of a specified content").

Claim 1's "essentially result-focused, functional character" confirms it is "ineligible under § 101." *Elec. Power Grp.*, 830 F.3d at 1356. The claim recites "identifying at least one regularly identifiable expression," "identifying at least a portion of information," and "extracting the portion of information," but it does not limit how to achieve these functions, which read on human activity.

Claim 1 also fails to recite any "specific improvement to the way computers operate," *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016), or "overcome a problem specifically arising in the realm of computer networks," *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014). Although the specification alleges that "regular-expression technology enables extremely fast pattern matching and information extraction with highly optimized standard programs" and "without the expensive and time consuming step of gathering and annotating a large 'training' database" (Dkt. No. 1-1 at 2:28–33), this is merely the "improved speed or efficiency inherent with applying the abstract idea on a computer" (*Customedia Techs., LLC v. Dish Network Corp.*, 951 F.3d 1359, 1364–65 (Fed. Cir. 2020) (quotations omitted)).

The same analysis applies to all other asserted claims, which Taasera admits are represented by claim 1. Ex. A at 29:22–24. The other independent claims (12, 23, 24, 25) recite the same steps of identifying expressions, identifying information, and extraction. Dkt. No. 1-1.

Two of these claims merely change the form of the invention from a "method" to an "apparatus" with a "memory . . . for storing" information (claim 12) and a "data capture device for obtaining the input sequence of data symbols" (claim 24). These same concepts were held abstract in *Content Extraction*. 776 F.3d at 1347 ("collecting" and "storing . . . data in a memory"). The other two independent claims reframe the same elements as an "article of manufacture" (claim 23) or add "comparing the input document to one or more previously-stored regular expressions" for a "match" (claim 25), which humans can also do. The dependent claims add nothing significant: the same mental step of "comparing" data to find a "match" (claims 2, 13); taking any "specified action" (claims 7, 18); and limiting data to categories including text (claims 10, 21). These elements do not make the claims less abstract and confirm that claim 1 is representative. *SAP*, 898 F.3d at 1167 ("collecting information, including when limited to particular content," is abstract).

B. *Alice* step two: the asserted claims fail to recite an inventive concept.

The '796 claims also fail *Alice* step two because "[t]hey add nothing outside the abstract realm." *SAP*, 898 F.3d at 1169. At most, some claims recite a "programming language," "processor," "memory," "data capture device," or "data output device" (claims 12, 24) but "require no improved computer resources [that the patentee] claims to have invented." *Id*. at 1169–70.

Indeed, the '796 patent admits that "'processor' . . . include[s] any processing device" (Dkt. No. 1-1 at 12:30–31); "'memory' . . . include[s] any memory devices associated with a processor" (*id*. at 12:35–37); "data capture device" can be a "digital scanner" or other "alternate forms" (*id*. at 11:49–65); and "data output device," whose "structure and operations depend on the application," can be any "display" (*id*. at 12:52–65). Again, "common programming languages" in the prior art had "built-in support for regular expressions" (*id*. at 2:25–27; *see also id*. at 3:22–31), and the claims "may be implemented in various forms of hardware, software, or combinations thereof," including "general purpose digital computers" (*id*. at 12:66–13:5). Thus, all asserted

claims fail both *Alice* steps. *Content Extraction*, 776 F.3d at 1348 ("recognizing and storing information from hard copy documents using a scanner and a computer" is not inventive).

II. The asserted claims of the '356 patent are patent-ineligible under § 101.

A. *Alice* step one: the asserted claims are directed to the abstract idea of sorting packets of data based on simple if/then logic that was performed by humans.

The '356 patent also predates *Alice* and relates to sorting packets of data using simple Boolean logic—specifically, using a known algorithm that the patent admits was already applied by humans—and is analogous to a person sorting through their mailbox to discard junk mail.

As background, the patent describes its invention as "automatically determining if a packet [of data in a network] is a new, exploit candidate." Dkt. No. 1-3 at 3:11–13. The patent explains that new exploit candidates were previously identified using a "honeypot," i.e., a network-connected device that is "not serving any useful function" besides receiving unsolicited packets. *Id*. at 2:38–50. The patent admits "[i]t is known for a human analyst to analyze all of the packets received by the honeypot" to determine if they are new exploit candidates: the human "analyst will determine which packets are harmless broadcast traffic, network administration, or web crawler requests" (which are not exploits); and the human "analyst will also look for harmful known viruses, worms, and exploitation code contained in the packets" (which are not "new" exploits). *Id*. at 2:50–57. Claim 1 recites "[a] computer program" automating these same steps:

> 1. A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:
> a computer-readable tangible storage device;
> first program instructions to ***determine if the packet is a known exploit***;
> second program instructions to ***determine if the packet is addressed to a broadcast IP address of a network***;
> third program instructions to ***determine if the packet is network administration traffic***;
> fourth program instructions, responsive to ***the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic,*** to determine that ***the packet is not a new, exploit candidate***; and
> fifth program instructions, responsive to ***the packet not being a known exploit AND***

> ***the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign,*** to determine and report that ***the packet is a new, exploit candidate***; and wherein
>
> the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device.

Id. at claim 1 (emphasis added). As in the prior human method, the packets of data may be "received by a honeypot" (*id*. at claim 5, which depends from claim 1), as set forth in the preferred embodiment. *Id*. at 4:23–25; *see also id*. at 3:51–4:11. Thus, claim 1 determines three conditions, which are the same conditions that human analysts previously determined: (i) "if the packet is a known exploit"; (ii) "if the packet is addressed to a broadcast IP address of a network"; and (iii) "if the packet is network administration traffic." *Id*. at claim 1; *see also id*. at 2:50–57. Using simple Boolean logic, if ***any*** condition is met, the packet is ***not*** a new exploit candidate. Conversely, if all three conditions are ***not*** met, the packet ***is*** a new exploit candidate.

Claim 1 is directed to the abstract idea of sorting data—i.e., classifying a packet as either a new exploit candidate or not a new exploit candidate—based on simple if/then logic. Thus, "with the exception of generic computer-implemented steps, there is nothing in the claims themselves that foreclose them from being performed by a human." *Symantec*, 838 F.3d at 1318. The Federal Circuit has compared similar data-sorting claims to the "long-prevalent practice for people receiving paper mail to look at an envelope and discard certain letters . . . based on characteristics of the mail," as "[t]he list of relevant characteristics could be kept in a person's head." *Id*. at 1314. Again, moreover, claim 1 merely automates the same manual process that humans previously performed to sort packets (Dkt. No. 1-3 at 2:50–57), and "mere automation of manual processes using generic computers does not constitute a patentable improvement in computer technology." *Credit Acceptance Corp. v. Westlake Servs*., 859 F.3d 1044, 1055 (Fed. Cir. 2017).

Claim 1 is similar to those invalidated in *Intellectual Ventures I LLC v. Erie Indemnity Co.*,

which claimed "a method for 'identifying and characterizing' files based on one of three selection criteria." 711 F. App'x 1012, 1015 (Fed. Cir. 2017). After selecting a file, the claims "characterize[ed] the file as an unauthorized file" if certain conditions were met. *Id*. at 1014. These claims were "directed to the identification of unwanted files in a particular field (i.e., a computer network) and otherwise concern data collection related to such identification, such that they are directed to an abstract idea." *Id*. at 1015. Here, as in *Erie*, there is no evidence that the steps "of selecting errant files apply rules of selection in a manner different from those which humans used, albeit with less efficiency, before the invention." *Id*. at 1016. A computer may be faster than a human (Dkt. No. 1-3 at 2:66–3:2), but that merely reflects the "efficiency inherent with applying the abstract idea on a computer" (*Customedia*, 951 F.3d at 1365).

Further confirming that claim 1 is abstract, each of its steps merely recites "a desired function or outcome, without providing any limiting detail that confines the claim to a particular solution to an identified problem." *Affinity Labs of Texas, LLC v. Amazon.com, Inc.*, 838 F.3d 1266, 1269 (Fed. Cir. 2016). Each step generically recites "program instructions" that "determine" if conditions are met, without limiting how any of the claimed determinations are made.

The other asserted independent claims (9–10, 13, and 17) are equally abstract. Claim 17 merely reframes the same steps into a generic "computer system" with "one or more processors," "memories," and "storage devices" (*id*.), but such "mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention" (*Alice*, 573 U.S. at 223). The remaining independent claims recite more "determin[ations]" and corresponding if/then statements, which are abstract mental steps. Dkt. No. 1-3.[2] The dependent claims tack on more

[2] Claim 9 ("determine if the packet has a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic"); claim 10 ("determine if the packet is network administration traffic by comparing an IP protocol and IP address of the packet to a list of

data collection and analysis steps: determining if the packet is "web crawler traffic" (claims 2, 14, 18); searching or determining a "signature" (claims 3, 6, 20); comparing "identities" (claim 4); using a honeypot (claim 19); comparing IP addresses (claims 8, 16); and processing a "sequence of packets" (claims 12, 15). Thus, all asserted claims are represented by claim 1 and are abstract.

B. *Alice* step two: the asserted claims fail to recite an inventive concept.

The claims fare no better at step two. Other than mental steps of "determin[ing]" conditions and classifying packets, the independent claims recite a generic "computer program product" with "a computer-readable tangible storage device" and generic "program instructions" (claims 1, 9–10, 13) or a "computer system" with generic "processors," "memories," and "storage devices" (claim 17). These elements, which "merely require generic computer implementation, fail to transform th[e] abstract idea." *Alice*, 573 U.S. at 221; *see id*. at 226 (elements for "a computer system and a computer-readable medium fail for substantially the same reasons," as do "data processing system" and "data storage unit"). As for the "determin[ing]" steps (claims 1, 9–10, 13, 17), they are in the abstract realm and provide no inventive concept, "no matter how ground-breaking" (*SAP*, 898 F.3d at 1170). Regardless, the patent admits these steps were conventional—it was "known for a human analyst to analyze all of the packets . . . to determine their type and whether they represent a known or unknown computer attack." Dkt. No. 1-3 at 2:50–66.

The same is true for the elements in the dependent claims—e.g., checking for web crawler traffic, packet signatures, using a honeypot, and processing packet sequences, all of which were admittedly conventional. *Id*. at 2:53–55 (known to "determine which packets are . . . web crawler requests"); *id*. at 1:40–59, 2:21–37, 6:64–67 (known to search and compare packet signatures); *id*.

---

combinations of IP protocols and IP addresses previously determined to be network administration traffic"); claim 13 ("determine if the packet has a protocol listed in a list of protocols previously determined to be harmless broadcast traffic").

at 2:38–39 ("A 'honeypot' is currently known to collect suspicious Internet message packets."), *id*. at 4:28–32 ("honeypot" can be a conventional computer); *id*. at 7:36–38 ("There are currently known methods that can identify which TCP packets are part of the same sequence and to reassemble these packets into the sequence."). Thus, the asserted '356 claims are all invalid.

III. The asserted claims of the '517 patent are patent-ineligible under § 101.

A. *Alice* step one: the asserted claims are directed to the abstract idea of assigning a score based on risk using rules and policies that are generic and undefined.

The '517 patent's asserted claims recite an abstract framework for managing a security policy, without reciting any technological improvement. Claim 1—one of only two independent claims—recites a method for (i) storing "rules" that correspond to an "action sequence"; (ii) storing "assessment policies"; (iii) identifying "a runtime risk"; and (iv) identifying "a behavior score":

> 1. A method for assessing runtime risk for an application program that executes on a device, comprising:
> ***storing***, in a rules database, a plurality of ***rules***, wherein each rule identifies an action sequence;
> ***storing***, in a policy database, a plurality of ***assessment policies***, wherein each assessment policy includes at least one rule of the plurality of rules;
> ***identifying***, using at least one assessment policy, ***a runtime risk for an application program that*** executes on a device, wherein the identified runtime risk ***indicates a risk or threat of the identified action sequence*** of the application; and
> ***identifying***, by a runtime monitor including a processing device, ***a behavior score for the application program*** that executes on the device based on the identified runtime risk, wherein
> the action sequence is a sequence of at least two performed actions, and
> each performed action is at least one of: a user action, an application action, and a system action.

Id. at claim 1 (emphasis added).

Claim 1 is directed to the abstract idea of assigning a score based on risk. The claim assigns the "runtime risk," and ultimately the "behavior score," based on known (but unspecified) "rules" and "policies," which could be assessed mentally by a human. Humans routinely assign scores based on rules to assess risk, such as credit ratings/scores, insurance rates, and medical prognoses.

Claim 1 is similar to those invalidated in *Dropbox, Inc. v. Synchronoss Technologies, Inc.*, which were directed to abstract ideas including "associating a security level with a data resource." 815 F. App'x 529, 532 (Fed. Cir. 2020). Like the '517 patent's "runtime risk" and "behavior score," the claim in *Dropbox* recited an "access checker" that invoked "a sensitivity level" and "a trust level" in deciding whether to grant access to computer resources (*id*. at 532), which the Federal Circuit held "offers nothing but a functional abstraction" (*id*. at 533). *See also Cisco Sys., Inc. v. Uniloc 2017 LLC*, 813 F. App'x 495, 497 (Fed. Cir. 2020) (invalidating claims "directed to the abstract idea of ranking stations based on antenna performance characteristics") (quotation omitted); *SmartGene, Inc. v. Advanced Biological Labs., SA*, 555 F. App'x 950, 952 (Fed. Cir. 2014) (invalidating claims that invoked "plurality of expert rules" to generate "a ranked listing").

Confirming that claim 1 is abstract, it does not limit how the claimed method must "identify[]" the "runtime risk for an application program" or the "behavior score for the application program." Dkt. No. 1-5 at claim 1; *Elec. Power Grp*., 830 F.3d at 1356. Nor does it recite any improvement to computer functionality or solve a computer-specific problem. The only steps relate to "storing" and "identifying" information. The claim does not require doing anything with this information, let alone in a way that provides a "specific asserted improvement in computer capabilities," as opposed to "computers . . . invoked merely as a tool." *Smart Sys. Innovations, LLC v. Chicago Transit Auth*., 873 F.3d 1364, 1372 (Fed. Cir. 2017) (quotations omitted).

The only other independent claim—claim 13—simply restates the same steps in the context of a "system." *Compare* Dkt. No. 1-5 at claim 1 *with id.* at claim 13. The dependent claims also add nothing material. Claims 2–5 and 14–17 limit the "actions" in the "action sequence" assessed for runtime risk (Dkt. No. 1-5), but such "limitation of the claims to a particular field of information—here, [actions evaluated for risk]—does not move the claims out of the realm of

abstract ideas." *SAP*, 898 F.3d at 1169. Claims 12 and 24 add a step of "assessing" whether actions "describe a forensic chain of events," but nothing prevents this from being performed by a human. Thus, claim 1 is representative of all asserted claims, which are abstract.

B. *Alice* step two: the asserted claims fail to recite an inventive concept.

None of the '517 patent's asserted claims recite an inventive concept. The "rules," "policies," "runtime risk," "behavior score," and "actions" are all in the abstract realm. *SAP*, 898 F.3d at 1168. While the claims recite a "device," "database[s]," and "processing device," these generic elements are insufficient. *Id*. at 1169–70 ("Some of the claims require various databases and processors," but these "require no improved computer resources"). Moreover, the '517 patent admits that no specialized technology is needed to practice the claims, and "other configurations or systems for performing the functions disclosed may be suitable." Dkt. No. 1-5 at 2:43–54; *see also id*. at 2:58–62. Thus, all asserted claims of the '517 patent fail both steps of the *Alice* test.

IV. The asserted claims of the '038 and '918 patents are patent-ineligible under § 101.

A. *Alice* step one: the asserted claims are directed to the abstract idea of determining compliance with a policy and restricting access to resources.

The '038 and '918 patents are related and share a common specification. The specification admits that the claims recite "methods and systems for controlling access to computing resources based on known computing security vulnerabilities" (Dkt. No. 1-6 at 1:22–25; *see also id*. at 3:36–38), which is an abstract idea. *See Ericsson Inc. v. TCL Commc'n Tech. Holdings Ltd.*, 955 F.3d 1317, 1326 (Fed. Cir. 2020) (invalidating claims "directed to the abstract idea of controlling access to, or limiting permission to, resources" using a "security access manager"). As the Federal Circuit has explained, determining or conditioning access on compliance with a policy "is pervasive in human activity, whether in libraries (loaning materials only to card-holding members), office buildings (allowing certain employees entrance to only certain floors), or banks (offering or

denying loans to applicants based on suitability and intended use)." *Id*. at 1327.

Here, the claims purport to control "remote electronic access to [ ] networks and computing resources, typically referred to as endpoint access control." Dkt. No. 1-6 at 1:53–55. Claim 1 of the '038 patent below recites a generic method to monitor endpoints for compliance:

> 1. ***A method for controlling the operation of an endpoint***, comprising:
> providing ***a user interface***, at a computing system remote from the end point, ***configured to allow configuration of a plurality of policies***;
> ***maintaining the plurality of policies in a data store*** on the computing system;
> ***identifying***, from the plurality of policies, a plurality ***of operating conditions*** on the endpoint to monitor;
> ***configuring*** one or more ***software agents*** on the endpoint ***to monitor the plurality of operating conditions***;
> ***receiving***, across a network, at the computing system, ***status information*** about the plurality of operating conditions on the endpoint gathered by the one or more software agents;
> ***determining***, by the computing system, ***a compliance state of the endpoint*** based on the status information and a plurality of compliance policies in the data store; and
> ***initiating***, by the computing system, ***based on the compliance state, an action identified in at least one rule*** in the data store, wherein the action is carried out by a processor on the endpoint.

Id. at claim 1 (emphasis added). Claim 1 of the '918 patent merely replaces the final "initiating" step (*id*.) with "authorizing access by the endpoint to a computing resource . . . in response to the compliance state; and continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes" (Dkt. No. 1-9 at claim 1).

These claims are directed to the abstract idea of determining compliance with a policy and (for the '918 patent) restricting access to resources. "[W]ith the exception of generic computer-implemented steps," this could be "performed by a human." *Symantec*, 838 F.3d at 1318. Claims 1 of the '038 and '918 patents are similar to those invalidated in *Ericsson*, which recited "receiving a request . . . to access the software services" and "determining if the request should be granted" based on "access and permission policies." *Id*. at 1326–27. "Although written in technical jargon," the claims were "directed to the abstract idea of controlling access to, or limiting permission to,

resources." *Id*. at 1326; *see also In re Gale*, 856 F. App'x 887, 889 (Fed. Cir. 2021) (invalidating claims "directed to the abstract idea of (1) collecting information (here, receiving messages and reading their metadata), (2) analyzing the information (here, calculating a usage pattern and determining its compliance with a predetermined usage pattern), and (3) reporting the results").

Moreover, nothing limits how the "software agents . . . monitor the plurality of operating conditions," how they determine "status information about the plurality of operating conditions," or how the system "determin[es] . . . a compliance state of the endpoint." Thus, as in *Ericsson*, the claims do not recite "a specific technique for improving computer performance" under *Enfish* or *DDR* because the claims "are silent as to how access is controlled." 955 F.3d at 1328.

The other independent claims recite the same process in the form of "[a] non-transitory computer readable medium" ('038 claim 12; '918 claim 9) or a "system" ('038 claim 23; '918 claim 17) but are otherwise identical. And like claim 1 of the '918 patent, claims 2, 13, and 24 of the '038 patent require "controlling access of the endpoint to computing resources" (Dkt. No. 1-6), which is an abstract idea (*Ericsson*, 955 F.3d at 1326). Most other claims recite variations on determining compliance with a policy.[3] They merely limit analyzed data to "a particular field of information," which is immaterial. *SAP*, 898 F.3d at 1169. The other claims recite more conventional components: a "web page" ('038 claims 3, 14, 25; '918 claims 2, 10, 18); "mobile device" ('038 claims 5, 16, 27; '918 claims 4, 12, 20); "servers" ('038 claims 10, 21, 32; '918 claims 8, 16, 24); and "software agents" provided by the operating system ('038 claims 6, 17, 28) or endpoint applications ('038 claims 7, 18, 29). Thus, all asserted claims are abstract.

[3] Such claims recite requesting "status information on a periodic basis" ('038 claims 4, 15, 26; '918 claims 3, 11, 19); monitoring a "hardware condition" ('038 claims 8, 19, 30; '918 claims 6, 14, 22) or "software condition" ('038 claims 9, 20, 31; '918 claims 7, 15, 23); having "at least one policy" that includes a rule identifying an action ('038 claims 11, 22, 33); and configuring endpoint applications to "monitor at least a subset of the . . . operating conditions" ('918 claims 5, 13, 21).

B. *Alice* step two: the asserted claims fail to recite an inventive concept.

The claims also fail *Alice* step two. Apart from the recited categories of information, which are in the abstract realm (e.g., "policies," "rules," "operating conditions," "status information," "compliance state[s]"), the computer and network components are all conventional. The independent claims recite an "endpoint"—a catch-all term for "remote electronic access" from another device. Dkt. No. 1-6 at 1:53–57; *see id*. at 7:52–64 ("endpoint system" can be "any processing system" made up of "conventional components"). The claims also recite a "computing system," "data store," "software agents [or services]," "network," and "processor" (e.g., Dkt. No. 1-6 at claim 1; Dkt. No. 1-9 at claim 1), but these invoke only "already available computers" (*SAP*, 898 F.3d at 1169–70) that were conventional and are used in the claims in their conventional manner. *See* Dkt. No. 1-6 at 1:30–43 (network connections "are ubiquitous in the industry and well known to the reader"), 7:24–29 (using, "in a conventional manner, a processor" and "conventional storage components"), 9:6–9 (using "the accepted definition in the art" for software agents), 59:6–7 ("conventional data communications network"). The generic elements in the dependent claims—i.e., "web page" ('038 claims 3, 14, 25; '918 claims 2, 10, 18), "mobile device" ('038 claims 5, 16, 27; '918 claims 4, 12, 20), "servers" ('038 claims 10, 21, 32; '918 claims 8, 16, 24), and software agents within the operating system ('038 claims 6, 17, 28) or endpoint applications ('038 claims 7, 18, 29)—are also conventional and used in a conventional manner.[4]

Thus, all asserted claims fail both *Alice* steps and are invalid under § 101.

[4] *See* Dkt. No. 1-6 at 21:49–51 (listing "Web sites" that "[m]any computer hardware and software vendors are known to maintain"), 7:44 (known "mobile communications device"), 2:55 (known "network servers"), 8:4–8 ("server computer" is "conventional processing system"), 1:63–65 (admitting "first generation of endpoint access control included operating system services"), 2:15–16 (exemplary known software agents include "antivirus agents[] [and] anti-spyware agents").

Dated: April 6, 2023

Respectfully submitted,

By: */s/ Michael R. Rueckheim*

Kelly C. Hunsaker
KHunsaker@winston.com
Michael R. Rueckheim
(Texas State Bar No. 24081129)
MRueckheim@winston.com
WINSTON & STRAWN LLP
225 Shoreline Drive, Suite 520
Redwood City, CA 94065
Telephone: (650) 858-6500
Facsimile: (650) 858-6550

Melissa Richards Smith
(Texas State Bar No. 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: 903-934-8450
Facsimile: 903-934-9257

ATTORNEYS FOR DEFENDANT,
PALO ALTO NETWORKS, INC.

CERTIFICATE OF COMPLIANCE WITH THE COURT'S
35 U.S.C. § 101 MOTION PRACTICE ORDER

☐ The parties **agree** that prior claim construction is not needed to inform the Court's analysis as to patentability.

☒ The parties **disagree** on whether prior claim construction is not needed to inform the Court's analysis as to patentability

/s/ Michael R. Rueckheim
Michael R. Rueckheim

CERTIFICATE OF CONFERENCE

This is to certify that counsel has complied with the meet and confer requirement in Local Rule CV-7(h) and this Court's Standing Order Regarding Motions Under 35 U.S.C. § 101 and Accompanying Certifications in Cases Assigned to United States District Judge Rodney Gilstrap. A conference was conducted telephonically on December 19, 2022, between counsel for PAN, Michael Rueckheim, and counsel for Taasera, Joseph Mercadante, Jennifer Truelove, and Fred Fabricant. On the meet and confer, counsel for Taasera confirmed it opposes the present motion and believes claim construction is needed to inform the analysis of patent-eligibility. Taasera's counsel has confirmed its position has not changed since the parties' meet and confer. Discussions have conclusively ended in an impasse, leaving an open issue for the Court to resolve.

Dated: April 6, 2023

/s/ Michael R. Rueckheim
Michael R. Rueckheim

CERTIFICATE OF SERVICE

The undersigned herby certifies that on April 6, 2023, a true and correct copy of the forgoing DEFENDANT PALO ALTO NETWORKS, INC.'S PARTIAL MOTION TO DISMISS UNDER FEDERAL RULE OF CIVIL PROCEDURE 12(b)(6) was electronically filed via the Court's CM/ECF system, which sends notifications of such filing to all counsel of record who have consented to accept service by electronic means.

/s/ Michael R. Rueckheim
Michael R. Rueckheim